ED Smart Notifications Solution Architecture

Version: 5.5

Date: June 20, 2018

Project: IAPD

DOC ID:

Author: Adam Trahan

Contents

Revision History

Version	Revision Date	Implemented By	Reason
1.0	5/23/2018	Adam Trahan	Initial Document
5.0	6/20/2018	Jason Miller	Remediation post review
5.5	7/20/2018	Adam Trahan	Updated based on feedback and discussion with Melissa and Amy

Approvals

Organization	Name	Role
RIQI	Elaine Fontaine	Stakeholder – Business Owner, COO
RIQI	Charlie Dansereau	Stakeholder – IT
RIQI	Faye Howard	Stakeholder – Operations
RIQI	Michael Dwyer	Stakeholder – Risk Management & Compliance

Contacts

Organization	Responsibilities	Contact(s)
RIQI – Business Owner	Represents Sponsor of the program organization and is ultimately responsible for foreseeing that the program meets its overall objectives. Empowered to make decisions on behalf of the sponsor.	Elaine Fontaine, EFontaine@riqi.org
RIQI – Project Manager	Responsibility for the successful initiation, planning, design, execution, monitoring, controlling and closure of a project.	April Arnold, AArnold@riqi.org
RIQI – Analyst	Responsible for defining needs and recommending solutions that deliver value to stakeholders. Gather and document needs and the rationale for change, and to design and describe solutions that deliver value.	Andrea Levesque, ALevesque@riqi.org
RIQI – Integration Engineer	Responsible for architecture and implementation planning and execution.	Adam Trahan ATrahan@riqi.org

Related Documentation

ID	Title	Version	Notes
	Risk Prediction of Emergency Department Revisit 30 Days Post Discharge: A Prospective Study https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4231082/	2014; 9(11): e112944	Megan Ranney recommended predictive analytics tool: Published online 2014 Nov 13. doi: 10.1371/journal.pone.0112944

1 Documentation Roadmap and Control

1.1 Access Control

This document is proprietary and confidential.

1.2 Document Distribution

This document will reside in confluence and is downloadable by any authorized Rhode Island Quality Institute employee or contractor.

1.3 Purpose and Scope

The purpose of this document is to educate authorized person on the software architecture and significant use cases for the Emergency Department Smart Notifications; A product of Rhode Island Quality Institute.

1.4 Process for Updating this Document

This document has been created by Adam Trahan. Any requests for changes to this document shall be emailed to the author at atrahan@riqi.org.

1.5 Relationships to other documents

This document, the software architecture document, defines the architecture of the overall solution. The Business Requirement Documents contains additional information about the solution.

1.6 How this document is organized

This Software Architecture Document is comprised of the following sections:

- Architecture Background identifies the background of the platform.
- Architecture Constraints identifies the constraints of the architecture.
- Technical Requirements identifies the functionality that the architecture must support.
- Architecture View identifies the architecture of the platform and discrete components.
- Use Case View identifies architecturally significant use cases and supporting sequence diagrams.
- Solution Options documents the potential systems that can support the architecture and needs of the platform.

1.7 Stakeholder Representation

The following table represents the stakeholders of the ED Smart Notifications project:

Role	Stakeholder	Email
Champion & Sponsor And Business Owner	Elaine Fontaine COO RIQI	efontaine@riqi.org
Project Manager	April Arnold, Manager, PMO RIQI	aarnold@riqi.org
Project Team Member	Andrea Levesque, Senior Customer Experience Manager RIQI	alevesque@riqi.org
Project Team Member	Greg Walker, Data Scientist RIQI	gwalker@riqi.org
Project Team Member	Caroline Muchui, Senior Interoperability Systems Engineer RIQI	cmuchui@riqi.org
Project Team Member	Adam Trahan, Senior Integration Engineer RIQI	atrahan@riqi.org
Project Team Member	Anthony Huntington, Senior Interoperability Systems Engineer RIQI	ahuntington@riqi.org
Project Team Member	Kelly Travis, Senior Business Operations Analyst RIQI	ktravis@riqi.org
Clinical Subject Matter Expert	Megan L. Ranney MD MPH FACEP Department of Emergency Medicine Alpert Medical School Brown University	megan_ranney@brown.edu

Role	Stakeholder	Email
Pilot Partner	Cedric J Priebe III Lifespan	Cedric.Priebe@Lifespan.org
Pilot Partner Project Contact	Brian Sousa Lifespan	bsousa@Lifespan.org
Subject Matter Expert	Neil Sarkar Brown Center for BioInformatics Brown University	neil_sarkar@brown.edu
Subject Matter Expert	Liz Chen Brown Center for BioInformatics Brown University	
Subject Matter Expert	Ira Wilson Department of Health Services, Policy, and Practice, School of Public Health Brown University	ira_wilson@brown.edu
Subject Matter Expert	Tom Trikalinos Department of Health Services, Policy, and Practice, School of Public Health Brown University	thomas_trikalinos@brown.edu
Subject Matter Expert	Chris Schmidt Department of Health Services, Policy, and Practice, School of Public Health Brown University	christopher_schmid@brown.edu
Funder/Stakeholder	Rhode Island Foundation	
Funder/Stakeholder	Amy Zimmerman HIT Co-ordinator Executive Office of Health & Human Services	amy.zimmerman@ohhs.ri.gov
Funder/Stakeholder	Melissa Lauer, MPA HIT Specialist Executive Office of Health & Human Services	Melissa.Lauer@ohhs.ri.gov
Funder/Stakeholder	Patrick Tigue RI Medicaid Director	
Stakeholder	Dr. James McDonald Rhode Island Department of Health	James.McDonald@health.ri.gov
Stakeholder	Dr. Nichole Alexander-Scott Director Rhode Island Department of Health	
Stakeholder	Marti Rosenberg Rhode Island State Innovation Model	Marti.Rosenberg@ohic.ri.gov

Role	Stakeholder	Email
Stakeholder	Brian Zink Chair, Department of Emergency Medicine, Alpert Medical School, Brown University	bzink@lifespan.org

1.8 Viewpoint Definitions and Documentation

This document contains the following two views of the solution: **Architecture View and Use Case View**.

2 Architecture Background

2.1 Business Goals, Objectives and Purpose

The ED Smart Notifications project has a goal to alert ED providers via EHR integration when a patient has a pre-determined condition, 1) risk of opioid use disorder or opioid overdose **and/or** 2) 7 and/or ED visit 30 day. Future projects can address other factors. These pre-determined conditions are evaluated based upon data analytics provided by RIQI utilizing data from multiple sources, such as CurrentCare data and the RI PDMP.

2.2 Users, Groups, Tasks and Task Profiles

2.2.1 Notification Recipient

A clinician user who views notifications from the HIE. The method of viewing is not closely defined for purposes of this document. This includes, but it not limited to a flag on a patient tracker within an EMR.

2.2.2 Data Consuming Partner (DCP)

An organization that has integrated with the ED Smart Notifications product to receive notifications by an electronic means.

2.3 Assumptions

1. RIQI will securely receive triggers (such as ADT messages) from the DCP which indicate the patient and event (such as an ED registration) to evaluate for notification(s). Triggers will include necessary demographic data to match or create new patient records where necessary.
2. RIQI will have a secure means to push notifications based on these triggers back to the DCP. The format and payloads of these notifications may vary depending upon the DCP's desired functionality. This includes, but is not necessarily limited to HL7v2 transactions.
3. The DCP will display these notifications to the clinical user in a prescribed manner.

2.4 Requirements Coverage

2.4.1 Environment and backup

The environment will be fully monitored and thresholds will be set to trigger when limits have been reached. All networking, storage, and VMware host are standard products and can be easily upgraded with proper notice.

All VM in current Production and Dev environments will have OS management services.

Active Watch service will be cover up to 75 Nodes for both Log and Threat Manager, and this includes Active watch service for both. The current Alert Logic Appliances will remain at each site.

The existing backup environment, which utilizes Evault was upgraded earlier this year, and will be utilized. Long term backups will continue to go to Evault, and short term backup for quick recovery will go to the onsite media vault.

We will be providing Enterprise Client Services Support which will include a TAM (Technical Account Manager) who will act as the project manager for the initial and subsequent implementations covering the scope of work to be fulfilled by TierPoint. As part of the services, TierPoint will have a dedicated support team that is persistent to RIQI.

The assigned Technical Account Manager (TAM) will provide project management services and works alongside the Service Delivery Consultant (SDC), who is a dedicated central technical resource, to provide persistent support to RIQI

These resources will be available between 8:30 a.m. and 5:30 p.m., Monday through Friday (ET), with emergency off-hours incident escalation. The TAM will conduct daily/weekly customer status meetings (frequency depends on requirements) and provide monthly service reports.

Environment will consist of:

Cisco 2960X – New Management Switch	Managed OS – Linux and Windows VM
5 Private Cloud Hosts (24/48 cores) Core Processors and 256 GB of RAM with 10G uplinks and utilizing the Shared FC network switching.	Windows standard Licensing for single hosts.
Additional VMware VCAN SP Advances Licensing, vCloud Director, vCloud Connector Advanced, NSX-SP Base (vCNS mode), vSphere Enterprise Plus, vCenter Server Standard	Managed Palo Alto SSG140
100MB ICX private circuit to connect Production to DR environment for Zerto Replication	Physical F-5 LB 2000S
RH Linux- Win OS Licenses	EMC Unity All Flash Array – 44TB
OS Management Windows / Linux	Alert Logic deployment
Windows / Linux Anti-Virus Managed Service	Uplink for Unity to shared FC switching.
Private Cloud Update Manager	VMware VCAN SP Advances Licensing, vCloud Director, vCloud Connector Advanced, NSX-SP Base (vCNS mode), vSphere Enterprise Plus, vCenter Server Standard
Technical Account Management and Service Delivery Consulting	Dual Cisco Nexus 5548 Switches 32 port

2.4.2 Disaster Recovery

A Private Cloud DRaaS (C2CR) is in place in order to meet the 80% of production performance requirements. This technology replicates the whole VM versus at the OS layer like current solution, which will allow for faster startup and better repeatability and less chance of errors.

A private cloud will be deployed with a single dedicated host, single network switch, single firewall, single VM for F5 Virtual load balancer, and single Unity 400F with 10.2TB of storage. This should properly run the production services with a 3.4:1 vCPU to pCPU ratio at current allocation.
The remote sites will establish VPN connection to turn on in case of a disaster if not already established.

DR environment

New Items (DR)
Cisco Nexus switching, 3172 Switching
Cisco 2960X
Uplink for Unity to shared FC switching.
100MB ICX private circuit to connect Production to DR environment for Zerto Replication
VMware VCAN SP Advances Licensing, vCloud Director, vCloud Connector Advanced, NSX-SP Base (vCNS mode), vSphere Enterprise Plus, vCenter Server Standard
Unix/Linux/Win OS Licenses and Management
Windows Anti-Virus Managed Service
DRaaS Base Package (Managed Cloud to Cloud Recovery)

DRaaS – Private Cloud Host (Large) – Dual Intel Xeon E5-2695v4 (36/72 cores) - 384 GB RAM - Quad-Port Embedded 1Gb Ethernet – 10G uplinks and Dual FC SAN connections
DRaaS VM License (Cloud to Cloud Recovery) -
DRaaS – STORAGE Unity 400F with 10 Drives, Usable Capacity 10.62TB, Effective Capacity 21TB , 8FC Ports
DRaaS – DUAL SAN Connection - (2) Managed Fibre Channel Switch Ports -

2.4.3 Monitoring and alert logic

The Ensemble service will monitor files transporting to the HealthShare instance. Additional monitoring is performed at various levels from within the application to the Operating System to the VMWare Hosts to the SAN. Monitoring entails observing message counts and activity, adapter integrity, application errors, OS resources, storage consumption, etc.

A scan detects and identifies network and host vulnerabilities in the RIQI environment and will therefore be layered into the ActiveWatch real-time review of security threats and alerts. Scans can perform external attack simulations as well as comprehensive vulnerability checks including registry evaluation. Server will be assigned to the CIDR range used by Alert Logic Threat Manager. The target server and any additional servers added to the environment shall be contained in CIDR range for *internal scan* runs from an Alert Logic appliance in the HealthShare environment. Scans shall specify credentials to use with the internal scan. Providing credentials, Threat Manager can log on to each host on the RIQI network and collect information about the host while it performs comprehensive vulnerability checks including registry setting evaluation. If RIQI does not provide credentials, Threat Manager scans the RIQI network without logging on to each host and performs as many checks as possible—but can have more false positives.

The following recommendations are adhered to with Threat Manager:

- Do not scan during service windows. Service windows are the times when RIQI does backups, hardware maintenance, or applies patches. Valid scan results require that the server is powered on and not in the middle of a reboot. For best results, scan *after* RIQI applies patches and not *while* applying patches.
- Scan Production environment during working hours. At night, laptops go home and workstations get powered off. Scan laptops and workstations when they are available on the RIQI network.

- Scan new computers before use. Scan new servers before the system is made available to the Internet.
- Do not scan during service windows.
- Make sure each scan is manageable.
    - Run open-ended scans.
    - Split up long scans into reasonable pieces.

2.4.4 Log Monitoring

The Environment shall be included in the Agent deployment for log monitoring. Log Manager automates log collection, aggregation and normalization, simplifying log searches, forensic analysis and report creation through real-time or scheduled analysis. Once logs are transferred to Alert Logic's secure cloud, Log Manager protects and stores the data to preserve against unauthorized loss, access or modification. LogReview is a second contracted service enhancement to Log Manager that provides daily event log monitoring and review, and is designed to help RIQI meet PCI DSS requirement 10.6. A team of certified security analysts acts as an extension of RIQI's team to expertly review your log data daily and alert you whenever suspicious activity or possible security breaches are detected. The LogReview case management system provides detailed, auditor-ready reports of detected incidents to demonstrate compliance with mandates related to log data review.

DDoS Mitigation – RIQI uses a multi-vector DDoS attack detection and mitigation solution designed to handle attacks at the network layer, server-based attacks, and application-layer DDoS attacks. The solution includes protection against volumetric and non-volumetric attacks, SYN flood attacks, low & slow attacks, HTTP floods, SSL-based attacks and more.

3 Architecture Constraints

The architecture constraints have affected and shaped the architecture of the RIQI Platform solution. The following constraints are detailed as follows:

3.1 Hardware and Operating System

There are no identified hardware constraints at this time.

3.2 Open Source Licensing

There are no acceptable open source constraints at this time.

4 Conceptual Architecture View

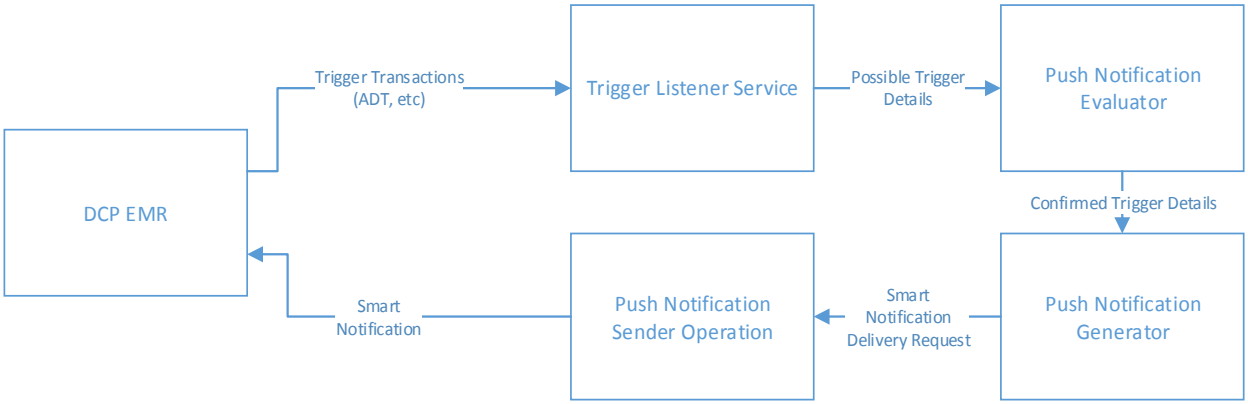

Figure 1 – Notification Conceptual Architecture

4.1 Data flow

Figure 1 shows a high level overview of the data flow through the ED Smart Notification architecture. The process begins with patient registration messages being sent from DCP into the HIE. When the messages are received, data from the message will be combined with other pieces of data to make several decisions about whether or not a flag/notification should be sent back to the DCP EMR. This decision making process will take place in the component labelled “Push Notification Evaluator”. This component will have access to the patient’s HIE information, and the calculated risk information from the Predictive model.

If a decision is made within the “Push Notification Evaluator” to send a notification, the process continues through to the “Push Notification Generator” and “Push Notification Sender Operation” components. These components manage the content within and the sending of the notification.

4.2 PDMP information

Within the “Push Notification Evaluator” step, a call to Appriss will be made to retrieve the prescription information for the patient. A web service will be called with patient and provider information. The Appriss API will take this information and then respond with information about the patient in the standard NCPDP format. Upon receipt of the response, the HIE will store this information so that it can be used in the calculations mentioned above.

4.3 Existing architecture

Figure 2 is being used to show that a majority of the existing components in the existing HIE architecture will either be involved or enhanced as part of this project.

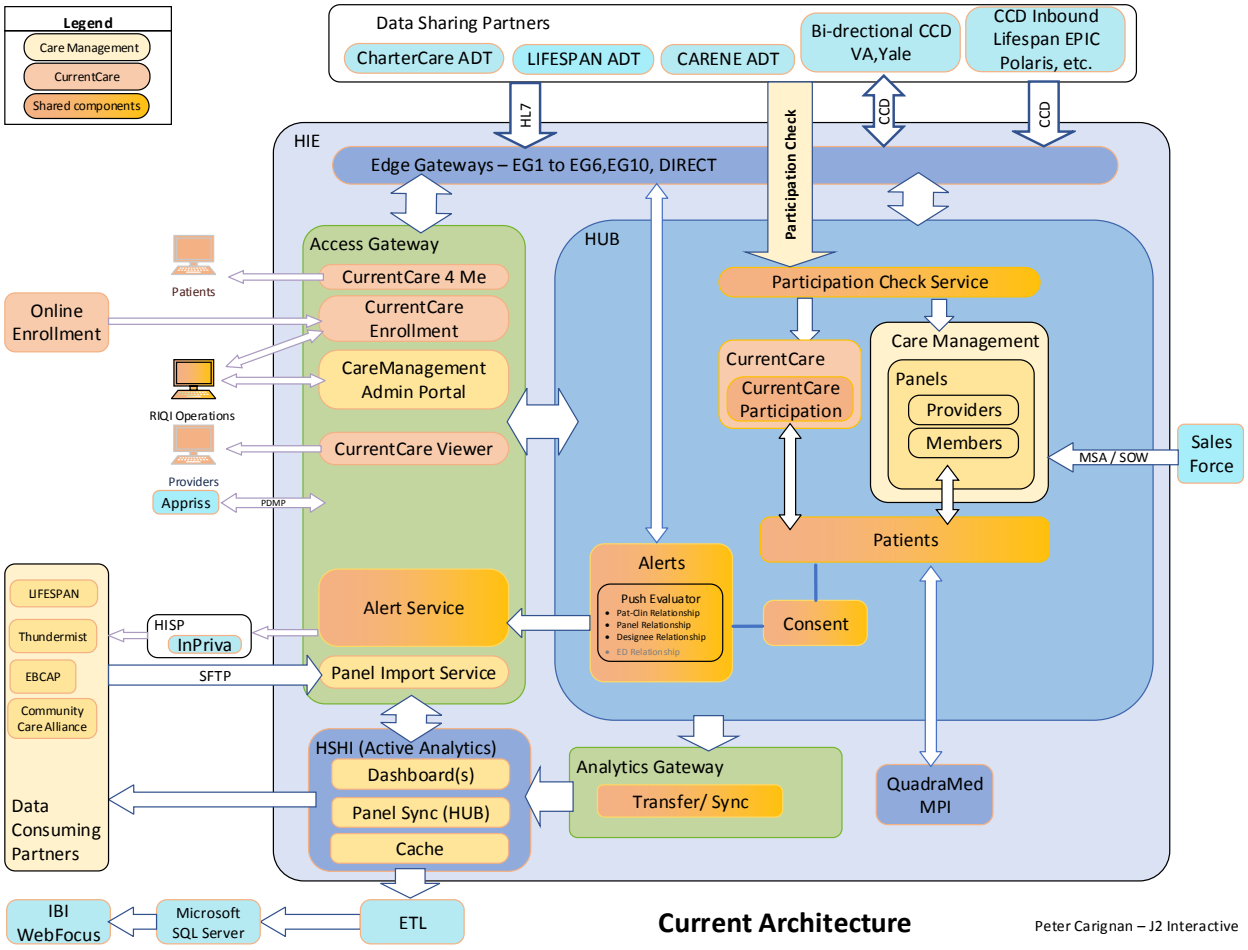

Figure 2: Component Architecture Diagram of RIQI HIE System

4.4 Dynamic Enrollment

A major enhancement that will allow all patients to be involved with EDSN is Dynamic Enrollment. The concept of dynamic enrollment uses an architecture similar to Care Management panels, but the patients are not associated to a specific provider. Dynamic Enrollment will allow the HIE to include non-Current Care and non-Care Management patients into the EDSN workflow.

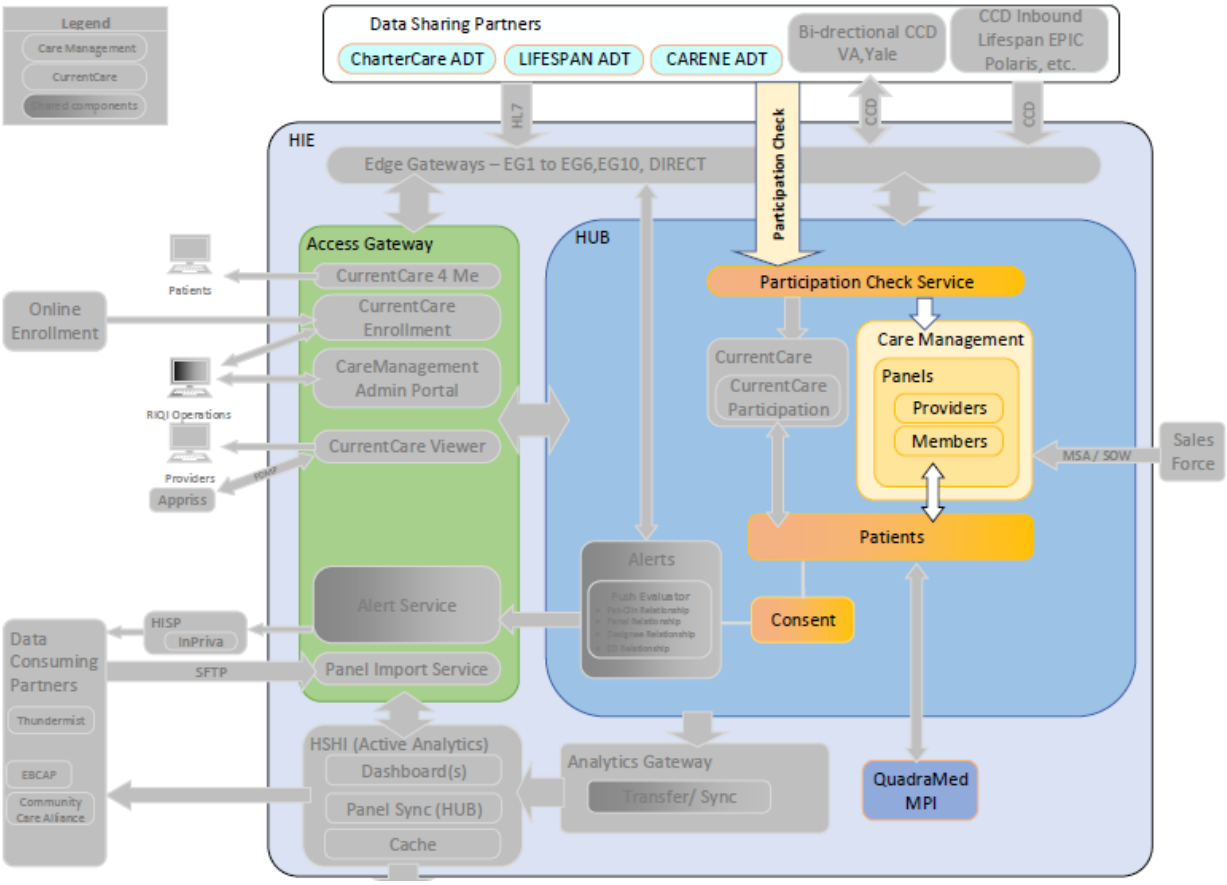

Figure 3: Component architecture diagram of dynamic enrollment

4.5 Outbound Push Architecture

Another major component being developed with the existing architecture is the Outbound Push Notification. This workflow is a major component of the project as it encompasses: (a) Receiving the ADT information from the DSP, (b) querying the relevant patient's HIE information, c) calculating risk information from the Predictive model to deduce if a notification should be sent, and (d) the generating of the content within and then the sending of the notification to the DCP's EMR system.

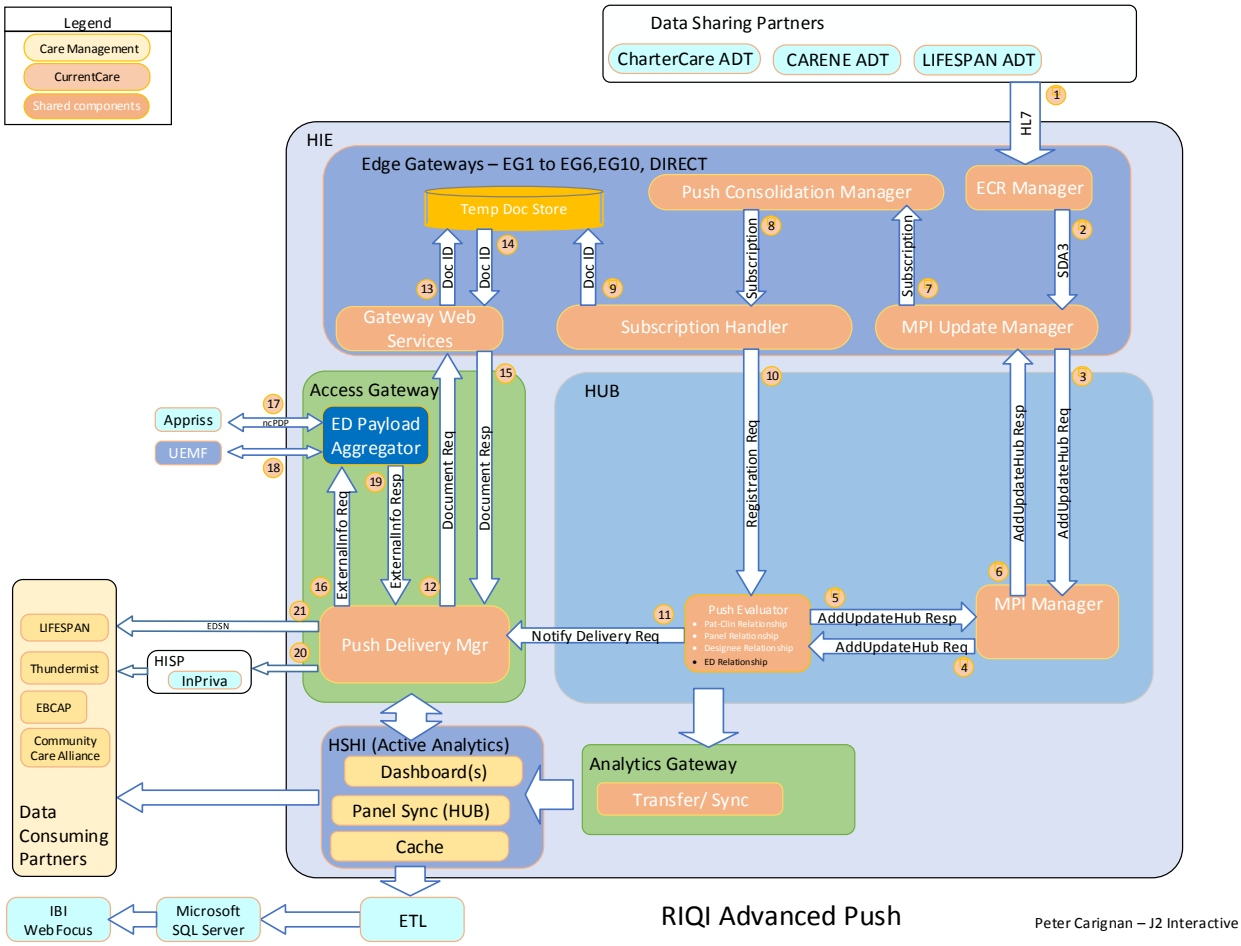

Figure 4: Component architecture diagram of outbound "push" architecture

5 Areas of Concern

1. Evaluation of notification depends upon analysis and implementation of an algorithmic function. Necessary clinical data must be available to accurately perform this.